FortiGate 80F Series



Highlights

Leader in the Gartner® Magic Quadrant™ for Hybrid Mesh Firewall

Unparalleled performance enabled by Fortinet's patented ASIC and the AI-enriched FortiOS operating system

Enterprise-grade protection with FortiGuard AI-Powered Security Services

Simplified operations with centralized management for networking and security, automated workflows, deep analytics, and self-healing

Inclusive SD-WAN and network controller in every FortiGate appliance at no extra cost

Rich portfolio for any business budget and need

Converged Next-Generation Firewall and SD-WAN

The FortiGate 80F series integrates firewalling, SD-WAN, network controller, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 80F series runs on FortiOS, a converged networking and security platform with secure AI controls and quantum-safe protection. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet solutions within a hybrid mesh firewall architecture.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate NGFW works seamlessly with FortiGuard AI-Powered Security Services to deliver coordinated, automated, end-to-end threat protection in real time.

The 80F family is built on the patented SD-WAN-based ASIC, which delivers unmatched performance over traditional CPUs with lower cost and reduced power consumption. This application-specific design and embedded multi-core processor further accelerate the convergence of networking and security functions in the 80F family to optimize secure connections and deliver a robust user experience at branch locations.

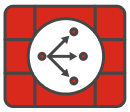
IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	900 Mbps	Multiple GE RJ45 | Variants with PoE, DSL, and/or storage

Use Cases



Perimeter Protection

- Protect networks from malicious traffic, guard against file-based threats, block web-based attacks, and secure applications and data with natively integrated FortiGuard AI-Powered Security Services
- Inspect and control incoming and outgoing traffic based on defined security policies
- Perform real-time SSL inspection (including TLS 1.3) with full visibility into users, devices, and applications across the attack surface
- Accelerate performance, protection, and energy efficiency with Fortinet's patented SPU with converged security and networking technologies



Secure SD-WAN

- FortiGate enables best-of-breed WAN edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN-based ASIC, delivers faster application identification to avoid delays in accessing applications and accelerates overlay performance regardless of location
- Enhances hybrid working with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with security service edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing



Secure Branch

- The Fortinet Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch secure Ethernet switches and FortiAP access points, FortiGate easily extends security to WAN, LAN, and WLAN at branch offices for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager to centralize visibility and simplify management across locations for IT teams
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions



Universal ZTNA

Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies.

- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System

FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

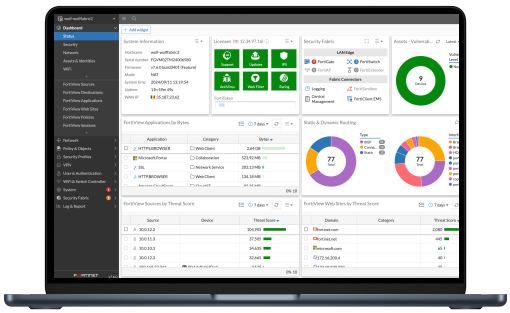
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios



Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status



FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR (optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

Zero-day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Unified Management for Optimal Security and Efficiency

Whether you are a small business or a large enterprise, Fortinet provides centralized control, visibility, and automation for your security infrastructure.

FortiManager: AI-powered, automation-driven, enterprise-class centralized management at scale

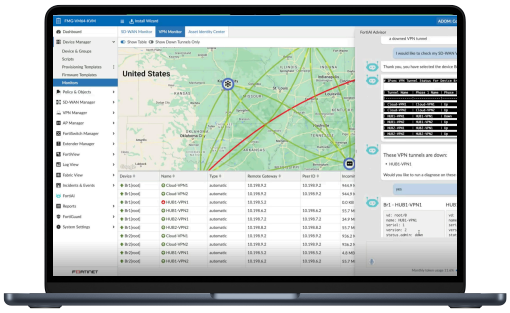
FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

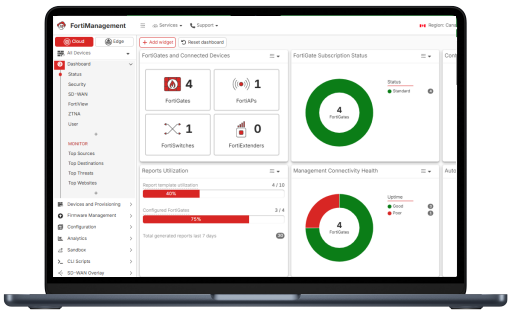
FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.

FortiManagement Cloud: Simplified management for small and mid-size businesses

FortiManagement Cloud is a SaaS service offering simplified management, security analytics, and reporting for Fortinet FortiGate NGFWs to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. It provides real-time and historical visibility into traffic analytics and security threats to reduce risks and improve security posture. View various threats, web traffic, and system events stored in the cloud for up to a year, with predefined reports to meet compliance and deliver actionable insights.



GenAI in FortiManager helps manage networks effortlessly -- generates configuration and policy scripts, troubleshoot issues, and execute recommended actions.



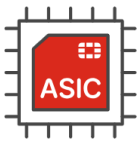
FortiManagement Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.

FortiConverter Service

Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

Fortinet ASICs: Unrivaled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

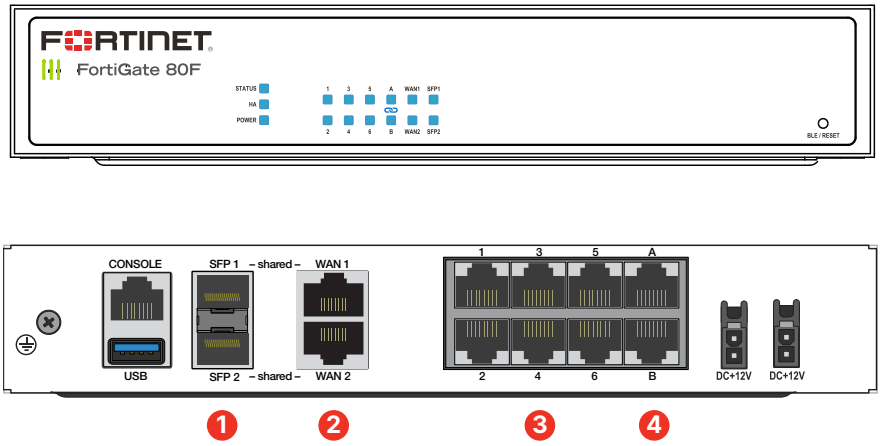
Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

Secure SD-WAN ASIC SP4

- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to the access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

Hardware

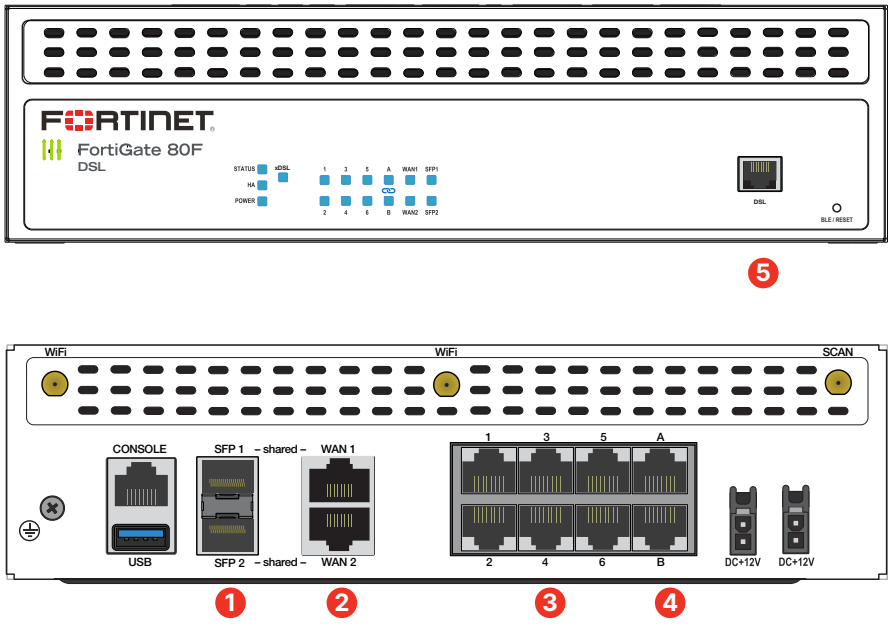
FortiGate 80F/81F



Interfaces

1. 2x GE RJ45/SFP Shared Media Ports
2. 2x WAN GE RJ45 Ports,
3. 6x GE RJ45* Ports
4. 2x GE RJ45* FortiLink Ports

FortiGate 80F-DSL and FortiGate 80F/81F-POE



Interfaces

1. 2x GE RJ45/SFP Shared Media Ports
2. 2x WAN GE RJ45 Ports,
3. 6x GE RJ45* Ports
4. 2x GE RJ45* FortiLink Ports
5. 1x DSL RJ11 Port (for 80F-DSL only)

* POE/+ ports for POE Variants

Hardware Features



Trusted Platform Module (TPM)

The FortiGate 80F series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.



Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.



Compact and reliable form factor

Designed for small environments, the FortiGate can be on a desktop or wall-mounted. It is small, lightweight, yet highly reliable with superior meantime between failures, minimizing the chance of network disruption.

Specifications

	FG-80F	FG-81F	FG-80F-POE	FG-81F-POE	FG-80F-DSL
Interfaces and Modules					
GE RJ45/SFP Shared Media Pairs	2	2	2	2	2
GE RJ45 Internal Ports	6	6	—	—	6
GE RJ45 FortiLink Ports (Default)	2	2	—	—	2
GE RJ45 PoE/+ Ports	—	—	6	6	—
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	2	2	—
DSL RJ11 Port	—	—	—	—	1
Wireless Interface	—	—	—	—	—
USB Ports 3.0	1	1	1	1	1
Console (RJ45)	1	1	1	1	1
Internal Storage	—	1× 128 GB SSD	—	1× 128 GB SSD	—
Trusted Platform Module (TPM)	✓	✓	✓	✓	—
Bluetooth Low Energy (BLE)	✓	✓	✓	✓	—
Signed Firmware Hardware Switch	—	—	—	—	—
System Performance — Enterprise Traffic Mix					
IPS Throughput [2]	1.4 Gbps				
NGFW Throughput [2, 4]	1 Gbps				
Threat Protection Throughput [2, 5]	900 Mbps				
System Performance and Capacity					
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	10 / 10 / 7 Gbps				
Firewall Latency (64 byte, UDP)	3.23 µs				
Firewall Throughput (Packet per Second)	10.5 Mpps				
Concurrent Sessions (TCP)	1.5 Million				
New Sessions/Second (TCP)	45 000				
Firewall Policies	5000				
IPsec VPN Throughput (512 byte)[1]	6.5 Gbps				
Gateway-to-Gateway IPsec VPN Tunnels	200				
Client-to-Gateway IPsec VPN Tunnels	2500				
SSL-VPN Throughput	950 Mbps				
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200				
SSL Inspection Throughput (IPS, avg HTTPS)[3]	715 Mbps				
SSL Inspection CPS (IPS, avg. HTTPS)[3]	700				
SSL Inspection Concurrent Session (IPS, avg HTTPS)[3]	100 000				
Application Control Throughput (HTTP 64K)[2]	1.8 Gbps				
CAPWAP Throughput (HTTP 64K)	9 Gbps				
Virtual Domains (Default / Maximum)	10 / 10				
Maximum Number of FortiSwitches Supported	24				
Maximum Number of FortiAPs (Total /Tunnel)	96 / 48				
Maximum Number of FortiTokens	500				
High Availability Configurations	Active-Active, Active-Passive, Clustering				

Note: All performance values are “up to” and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

	FG-80F	FG-81F	FG-80F-POE	FG-81F-POE	FG-80F-DSL
Dimensions and Power					
Height x Width x Length (inches)	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0
Height x Width x Length (mm)	40 × 216 × 178	40 × 216 × 178	60 × 216 × 178	60 × 216 × 178	60 × 216 × 178
Weight	2.4 lbs (1.1 kg)	2.4 lbs (1.1 kg)	3.1 lbs (1.4 kg)	3.1 lbs (1.4 kg)	3.07 lbs (1.39 kg)
Form Factor (supports EIA/non-EIA standards)	Desktop/ Wall Mount/ Rack Tray	Desktop/ Wall Mount/ Rack Tray	Desktop/ Wall Mount/ Rack Tray	Desktop/ Wall Mount/ Rack Tray	Desktop / Wallmount (optional)
Operating Environment and Certifications					
Input Rating	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)	12V DC, 5A
Power Required (Redundancy Optional)	Powered by up to two external DC power adapters (one adapter included), 100–240V AC, 50/60 Hz				
Maximum Current	115VAC/0.4A, 230VAC/0.2A	115VAC/0.4A, 230VAC/0.2A	115VAC/2.2A, 230VAC/1.1A	115VAC/1.2A, 230VAC/0.6A	115Vac/0.9A, 230Vac/0.6A
Total Available PoE Power Budget*	—	—	96W	96W	—
Power Consumption (Average / Maximum)	12.69 W / 15.51 W	13.5 W / 16.5 W	96 W / 118 W	98 W / 137 W	28.0 W / 31.6 W
Heat Dissipation	52.55 BTU/h	56.30 BTU/h	402.26 BTU/h	467.5 BTU/h	108 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)				
Storage Temperature	-31°F to 158°F (-35°C to 70°C)				
Humidity	10% to 90% non-condensing				
Noise Level	Fanless 0 dBA	Fanless 0 dBA	31.56 dBA	31.56 dBA	24.14 dBA
Operating Altitude	Up to 7400 ft (2250 m)				
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB				
Certifications	USGv6/IPv6				
xDSL Modem - Supported Mode					
VDSL2	—	—	—	—	✓
ADSL2	—	—	—	—	✓
ADSL2+	—	—	—	—	✓
G.DMT	—	—	—	—	✓
T1.413	—	—	—	—	✓
G.Lite	—	—	—	—	✓
xDSL Modem - Supported Type					
Annex A, B, I,J, M and L	—	—	—	—	✓

* Maximum loading on each PoE/+ port is 30 W (802.3at).

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection	Bundles: SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct, AI-based Heurestic AV, FortiGate Cloud Sandbox[1]	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video Filtering, Malicious Certificate[1]	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP)[2]	•	•			
	IoT Security — IoT Device Detection, IoT Vulnerability Correlation, and Virtual Patching[3]		•			•
	Security Rating (and Outbreak Check)[3]		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS[2]	•				
	Application Control	----------included with FortiCare Subscription----------				
	Inline CASB[1]	----------included with FortiCare Subscription----------				
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[4]					•
	One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•			
	Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management	•				
	FortiManagement Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium[3]	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing	----------included with FortiCare Subscription----------				

1. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Not available for SD-WAN Bundle SKU FC-10-XXXXX-1387-02-DD.
4. Only supported on FortiGate/FortiWiFi models from the 70F (F-series and all later series) and FGR-60G onwards. See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles offer curated security services to combat known, unknown, zero-day, and emerging AI threats. They protect against malicious content, web threats, and secure IT/OT/IoT devices, applications, users, and data. All bundles include FortiCare Premium Services with 24×7×365 support, one-hour critical response, and next-business-day noncritical response.

Fortinet's FortiCare Services support the Security Fabric throughout its lifecycle—Design, Deploy, Operate, Optimize, and Evolve. FortiCare Elite delivers enhanced SLAs, rapid issue resolution, dedicated support, 18 months of extended engineering support, and a unified portal for device and security health, improving operational efficiency and deployment performance.

Ordering Information

Product	SKU	Description
FortiGate 80F	FG-80F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports.
FortiGate 80F	FG-80F-HA	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 81F	FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 128GB onboard storage.
FortiGate 81F	FG-81F-HA	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 128GB SSD. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 80F-POE	FG-80F-POE	8 x GE PoE ports, 2 x RJ45/SFP shared media WAN ports.
FortiGate 80F-POE	FG-80F-POE-HA	8 x GE PoE ports, 2 x RJ45/SFP shared media WAN ports. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 81F-POE	FG-81F-POE	8 x GE RJ45 PoE ports, 2 x RJ45/SFP shared media WAN ports, 128GB SSD.
FortiGate 81F-POE	FG-81F-POE-HA	8 x GE RJ45 PoE ports, 2 x RJ45/SFP shared media WAN ports, 128GB SSD. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 80F-DSL	FG-80F-DSL	8 x GE RJ45 Ports, 2 x RJ45/SFP shared media WAN ports, with embedded DSL module.
FortiGate 80F-DSL	FG-80F-DSL-HA	8 x GE RJ45 Ports, 2 x RJ45/SFP shared media WAN ports, with embedded DSL module. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts.
Accessories	**SKU**	**Description**
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 70/71F, 70/71G, 80E/81E, 80/81F, 90/91G and FDC-100G. Power cable SP-FG60CPCOR-XX sold separately.
AC Power Adaptor	SP-FWF80F-PDC-5	Pack of 5 AC power adaptors for FG-80F-DSL, power cable SP-FGPCOR-XX sold separately.
AC Power Adaptor	SP-FG80E-POE-PDC	AC power adaptor for FG-60E-POE, FG-80E-POE, FG-81E-POE, FG-80/81F-POE, power cable SP-FG60CPCOR-XX sold separately.
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models.
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.
Transceivers	**SKU**	**Description**
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1GE SFP Transceiver, 90km Range, -40°/85°C Operation	FR-TRAN-ZX	1G SFP transceivers, -40°/85°C operation, 90km range for all systems with SFP Slots.

RC (regional code): A, B, D, E, F, I, J, N, P , S, V, and Y

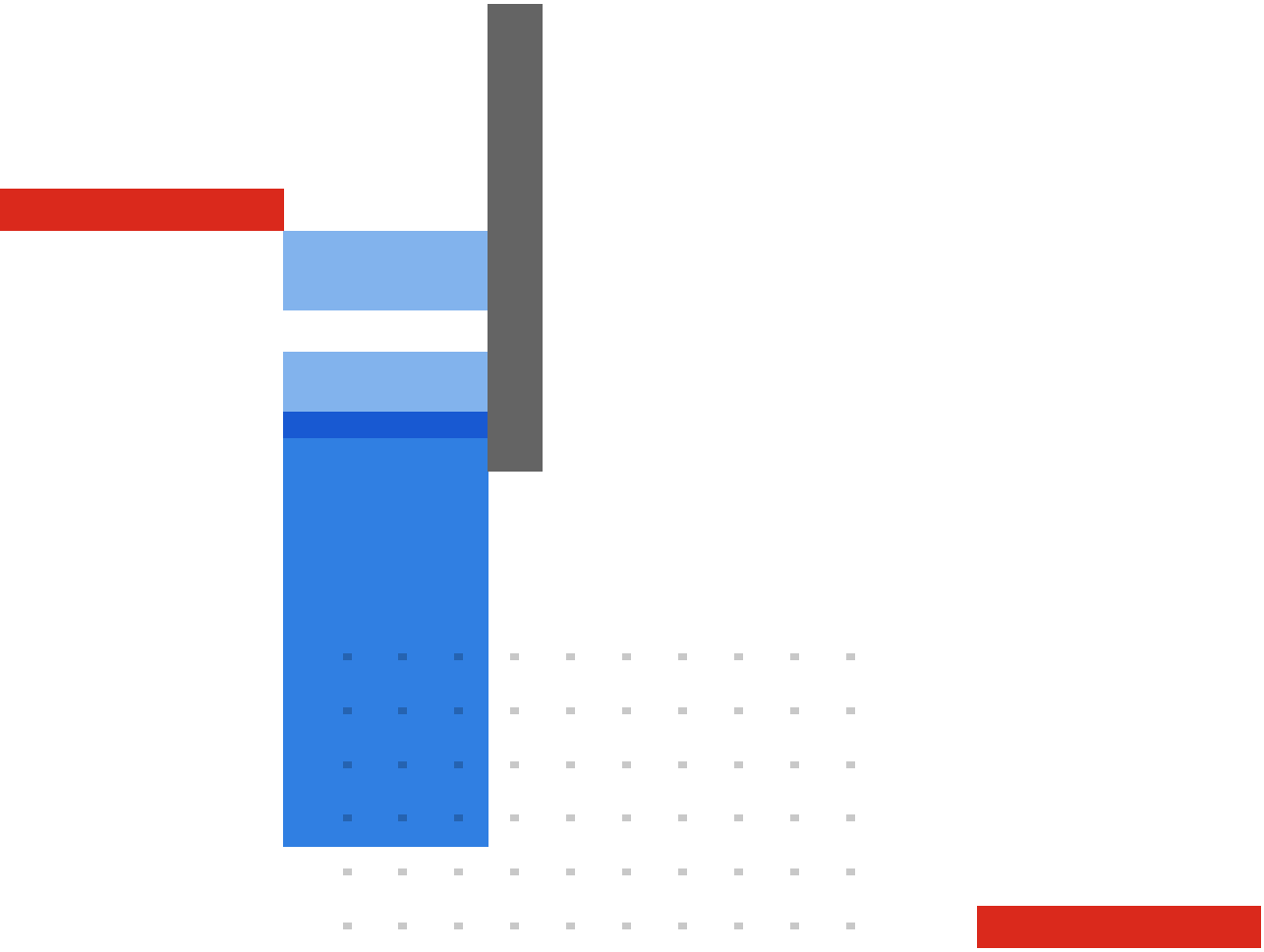
Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

For hard-coded firmware ceilings for a specific software version, visit: Maximum Values Table Tool.

The link to the max value table: https://docs.fortinet.com/max-value-table?product_family=fortigate&family=fortigate

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 1, 2026

FG-80F-DAT-R48-20261001